

MFA Set up Options

Multi-Factor Authentication (MFA), or sometimes referred to as 2FA (two-factor authentication), is a process of providing two pieces of identification as your credentials when logging in into your account. This means that whenever you need to access, either your CUE email, Online Services, or Moodle, you will need to provide something that you know (your password), and something that you have (eg., PIN code sent to your phone or a piece of hardware).

You can use one or any combination of the options presented on the next page to implement MFA on CUE services:

- [Option 1: Authenticator App](#)
- [Option 2: Hardware Token](#)

Option 1: Authenticator App

An authenticator app generates PIN codes on your phone for two-factor authentication. When logging in, you will enter your password and a PIN generated by your Authenticator app.

1. Download the Google Authenticator App (or similar OTP app) from the [Android Play Store](#) or the [Apple Store](#) onto your mobile device.
2. Login to Online Services for Faculty (<https://onlineservices.concordia.ab.ca/>) from another device, other than the phone where you have the Authenticator app.



3. Go to **My Account**.
4. Choose **Change password**.
5. In the *Multi-Factor Authentication* section, choose **Authenticator App**.

Phone Number	Description	Action
--------------	-------------	--------

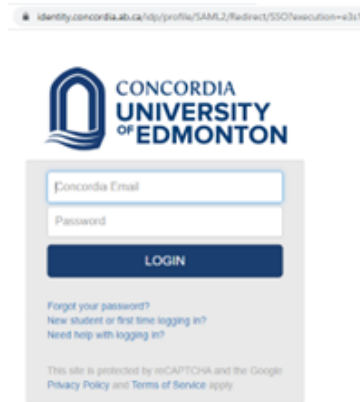
6. (Optional) Type in a Device description. Please make sure not to use the characters(" " or ") in your device description.
7. Click on **Add Device**. A QR code will be generated, which you will need to scan with the downloaded Authenticator app.
8. Upon successful scan, your CUE account will be setup in your app. A new 6-digit code will be generated by the app every 30 seconds. You will need to enter your password and the displayed 6-digit code on your app whenever you need to login to your CUE account.

Option 2: Hardware Token

(a video tutorial is also available [here](#))

A hardware token is an actual physical USB key that you plug into your computer/laptop that is used to authenticate your account. These devices are available at the CUE Bookstore.

1. Login to Online Services for Faculty (<https://onlineservices.concordia.ab.ca/>)

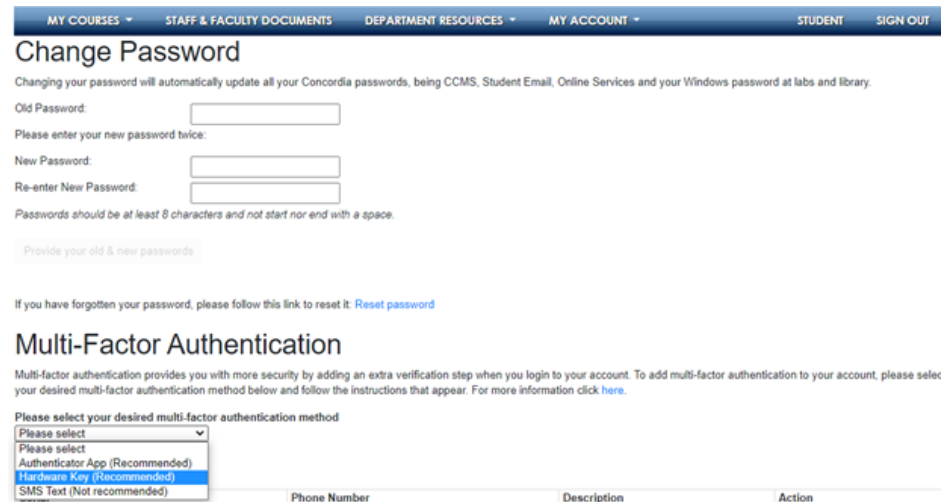


The image shows the login page for Concordia University of Edmonton. At the top is the university's logo. Below it is a login form with fields for 'Concordia Email' and 'Password', and a 'LOGIN' button. There are links for 'Forgot your password?', 'New student or first time logging in?', and 'Need help with logging in?'. At the bottom, it states 'This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.'



The image shows the footer of the Concordia University of Edmonton website. It includes the university's logo, the name 'Concordia University of Edmonton', and links for 'Shibboleth Single Sign-On Service' and 'Contact the IT Services Helpdesk'.

2. Go to **My Account**.
3. Choose **Change password**.
4. In the *Multi-Factor Authentication* section, choose **Hardware key**.



The image shows the 'Change Password' and 'Multi-Factor Authentication' sections of the Concordia University of Edmonton online services. The 'Change Password' section has fields for 'Old Password', 'New Password', and 'Re-enter New Password', with a note that passwords should be at least 8 characters and not start or end with a space. Below this is a 'Provide your old & new passwords' button. The 'Multi-Factor Authentication' section has a link to 'Reset password' and a dropdown menu to 'Please select your desired multi-factor authentication method'. The dropdown menu is open, showing options: 'Please select', 'Authenticator App (Recommended)', 'Hardware Key (Recommended)', and 'SMS Text (Not recommended)'. Below the dropdown is a table with columns 'Phone Number', 'Description', and 'Action'.

Phone Number	Description	Action
--------------	-------------	--------

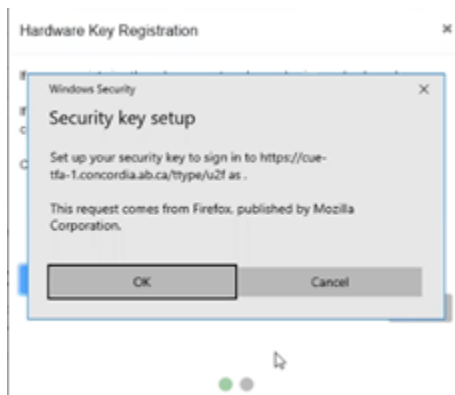
5. Click on **Add Device**.
 6. (Optional) On the next screen, type in a device description, then click on **Next**.
- Note:** Please make sure not to use the characters (" or ') in your device description.



The image shows the 'Hardware Key Registration' form. It has a title bar with a close button. Below the title, it says 'You can enter a device description in case you add multiple devices later and want to know which one is which.' There is a label 'Device Description (optional):' followed by a text input field. To the right of the input field is a blue 'Next' button. At the bottom, there are two small circles, one of which is filled, indicating the current step in a process.

7. Plug into a USB slot the hardware token device that you will use into your computer/laptop, and click on **Add Device**

8. Confirm the information displaying on your screen by clicking on **OK**.



9. Your hardware key should now begin flashing green. Touch the flashing circle on your hardware key.



10. Once you get the confirmation that hardware token has been registered to your device, click on **Close** to complete the set up.

If you have any questions please send them to helpdesk@concordia.ab.ca or call us at 780-479-9316.



Related articles

- [MFA Set up Options](#)
- [Set or Reset Password for Student Club or Role Account](#)
- [IT Orientation](#)

- [Wordpress Development Website Access Information](#)
- [Set Up Keepass](#)